01-03-00 A

Please type a plus sign (+) inside this box → +

PTO/SB/05 (4/98)
Approved for use through 09/30/2000. OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	042390.P6098
First Inventor or Application Identifier	Rodney A. Korn
Title	METHOD AND APPARATUS FOR CREATING AND EXECUTING
Express Mail Label No.	EL414969776US

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents

ADDRESS TO: Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

1. ☒ Fee Transmittal Form
(Submit an original, and a duplicate for fee processing)

2. ☒ Specification [*Total Pages* 15]
(preferred arrangement set forth below)
- Descriptive title of the Invention
- Cross References to Related Applications
- Statement Regarding Fed sponsored R & D
- Reference to Microfiche Appendix
- Background of the Invention
- Brief Summary of the Invention
- Brief Description of the Drawings (*if filed*)
- Detailed Description
- Claim(s)
- Abstract of the Disclosure

3. ☒ Drawing(s) *(35 U.S.C. 113)* [*Total Sheets* 2]

4. Oath or Declaration [*Total Pages* 4]
a. ☐ Newly executed (original copy)
b. ☐ Copy from a prior application (37 C.F.R. § 1.63(d)) *(for continuation/divisional with Box 16 completed)*
i. ☐ DELETION OF INVENTOR(S)
Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR §§ 1.63(d)(2) and 1.33(b).

5. ☐ Microfiche Computer Program *(Appendix)*

6. Nucleotide and/or Amino Acid Sequence Submission *(if applicable, all necessary)*
a. ☐ Computer Readable Copy
b. ☐ Paper Copy (identical to computer copy)
c. ☐ Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

7. ☐ Assignment Papers (cover sheet & document(s))
8. ☐ 37 C.F.R. § 3.73(b) Statement *(when there is an assignee)* ☐ Power of Attorney
9. ☐ English Translation Document *(if applicable)*
10. ☐ Information Disclosure Statement (IDS)/PTO - 1449 ☐ Copies of IDS Citations
11. ☐ Preliminary Amendment
12. ☒ Return Receipt Postcard (MPEP 503) *(Should be specifically itemized)*
13. ☐ *Small Entity Statement(s) ☐ Statement filed in prior application, Status still proper and desired
14. ☐ Certified Copy of Priority Document(s) *(if foreign priority is claimed)*
15. ☐ Other: .....

**NOTE FOR ITEMS 1 & 13: IN ORDER TO BE ENTITLED TO PAY SMALL ENTITY FEES, A SMALL ENTITY STATEMENT IS REQUIRED (37 C.F.R. § 1.27), EXCEPT IF ONE FILED IN A PRIOR APPLICATION IS RELIED UPON (37 C.F.R. § 1.28).*

16. If a CONTINUING APPLICATION, *check appropriate box, and supply the requisite information below and in a preliminary amendment:*
☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No: _____

Prior application Information: Examiner _____ *Group/Art Unit:* _____

For CONTINUATION or DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 4b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

17. CORRESPONDENCE ADDRESS

☐ *Customer Number or Bar Code Label* *(Insert Customer No. or Attach bar code label here)* *or* ☒ *Correspondence address below*

Name	BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP				
Address	12400 Wilshire Boulevard, Seventh Floor				
City	Los Angeles	State	California	Zip Code	90025
Country	U.S.A.	Telephone	(503) 684-6200	Fax	(503) 684-3245

Name (Print/Type)	Gregory D. Caldwell, Reg. No. 39,926		
Signature		Date	12/31/99

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

TITLE OF THE INVENTION:

Method and Apparatus for Creating and Executing Secure Scripts

INVENTOR:

RODNEY A. KORN

Prepared by

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1026
(408) 720-8300

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to the field of encryption. Specifically, the present invention relates to creating and executing secure, i.e., encrypted, scripts by a world wide web-enabled application.

Description of the Related Art

Present World Wide Web browsers, such as Internet Explorer, available from Microsoft Corporation, are limited by the constraints of the HyperText Mark-Up Language (HTML). Web content based on HTML comprises static, two dimensional text and graphics. A scripting language, such as JavaScript - a cross-platform, object-based scripting language for client and server applications developed by Netscape Communications, Inc., extends a Web browser's capabilities. A scripting language allows access to objects within the browser and supports execution of Web applications. A script, written in a scripting language, typically has access to browser objects in an HTML document or page, and is capable of modifying variables in the HTML document. Thus, the script extends the capabilities of HTML processing without requiring interaction with a HyperText Transfer Protocol (HTTP) server. The script typically is downloaded by the browser as part of an HTML page and is processed as the page is received, or when a browser event occurs, such as the click of a button on the HTML page.

A script differs from an applet. Although an applet also is downloaded as part of a Web page and run on a client system, the applet stands alone, that is, it is not part of the browser application, just as a an application program, such as a word processor application, is not part of an operating system.

In addition to scripts and applets, controls enhance Web browsers. For example, ActiveX controls are interactive objects in a Web page that provide interactive and user-controllable functions. ActiveX controls are part of a set of technologies available from Microsoft Corporation, based on a refinement of the well known COM standard, that is directed to enabling interactive content for Web pages. ActiveX currently is supported by the Microsoft Windows operating system, but will be supported on other platforms, such as the Macintosh platform available from Apple Computer, and UNIX platforms.

Without sufficient security mechanisms in place, it is possible to download a Web page that contains controls that launch an application that causes harm or unintended results, e.g., to the client system. Furthermore, if the controls are not secure, the provider of a Web site risks attack by computer hackers, and is vulnerable to software bugs.

BRIEF SUMMARY OF THE INVENTION

The invention provides a method for creating a secure script. Executable commands in the script are hashed, and the hashed values for the commands are encrypted and appended to the script.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention is illustrated by way of example and not limitation in the following figures. Like references indicate similar elements, in which:

Fig. 1 is a flow chart illustrating an embodiment of the invention.

Fig. 2 is a flow chart illustrating an embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

An embodiment of the present invention enables Web pages to execute software applications on a client system, e.g., a personal computer (PC), in a secure manner using a signed control, and a signed and encrypted script. Embodiments of the invention may be represented as a software product received over, and/or stored on, a machine-readable medium (also referred to as a computer-readable medium or a processor-readable medium). The machine-readable medium may be any type of magnetic, optical, or electrical storage medium including a diskette, CD-ROM, memory device (volatile or non-volatile), or similar storage mechanism. Moreover, the machine readable medium may accessed at a server by a client via a network connection between the client and server, for example, in a client/server computing environment. The machine-readable medium may contain various sets of instructions, code sequences, configuration information, or other data. For example, the procedures described herein can be stored on the machine-readable medium. Those of ordinary skill in the art will appreciate that other instructions and operations necessary to implement the described invention may also be stored on the machine-readable medium.

In one embodiment of the invention, a script in a World Wide Web page ("Web page", "Web document", or "HyperText Markup Language (HTML) document") is hashed and encrypted. A control in the Web page, such as ActiveX, decrypts and hashes the script to verify the script has not been altered or tampered with, before executing or causing to execute the script. In this manner, one can serve to a client web pages that contain interactive content or that execute local applications in a secure fashion. The described embodiment involves a script that may be invoked by a Web browser application, or more particularly, by a control in a Web page

downloaded by the Web browser application. However, it should be noted that any application or software program can benefit from the present invention to protect malicious modification of or hacking to a script or the like.

With reference to Fig. 1, the process starts at 110 with hashing the commands in the script. The script is written in a scripting language, such as JavaScript, and comprises executable commands to cause the client system upon which the script is executed to perform some function. The function may be defragmenting a hard disk drive accessible by the system upon which the script is executed, or providing interactive content in a Web page downloaded to a client system, e.g., online tutorial or help. The content of the script is not so important as is preventing unauthorized control of the script or unauthorized alteration of the script content in so much as an embodiment of the present invention is concerned.

Any well known or proprietary hashing function may be utilized to compute a hashed value for each executable command in the script. Each executable command is provided at 105 as the key value input to the hashing function, from which the hashing function computes a hashed value corresponding to the executable command. In one embodiment of the invention, each executable command may be hashed, while in other embodiments of the invention, some number of executable commands, e.g., one or more but less than all of the executable commands, may be hashed. In one embodiment of the invention, the hashing function utilizes public key A that is tied to the script, as described below, thus making it highly unlikely that the script was authored or edited by an unauthorized individual without access to the corresponding private key.

At 120, each hashed value is encrypted using well known asymmetric, i.e., public, key cryptography techniques. For example, each hashed value is encrypted using private key A 106.

This process is also referred to in cryptography as creating a public key digital signature. Public key digital signatures provide a way to prove that the signed data was signed by one who had a copy of a particular private key, in this case, private key A.

The signed hashed values for the executable commands are embedded or appended to the script at 130. Alternatively, the hashed values may first be appended to the script and then signed. A public key A corresponding to the private key A may be appended to the script as well, or obtained from the public key authentication infrastructure, e.g., a certification authority. (A public file known as a certificate is issued by the certification authority and contains an entity's public key, identifying information, and a signature provided by the certification authority). At 140, the script, including the signed hashed values and public key, if present, may be encrypted using a symmetric key 107 to provide a second level of encryption. The encryption is not necessary for protection of the script, but hides the public key, if included in the script.

In a Web-enabled application, the script, encrypted or not as the case may be, is converted as appropriate for inclusion in a Web page. The public key A 108 corresponding to the private key A 106 is provided to control, i.e., interactive objects that provide interactive and user-controllable functions, in the Web page. In one embodiment of the invention, the Web page utilizes ActiveX control from Microsoft Corporation. The control is also signed at 160, to hide public key A provided therein at 150. The control is signed using a different private key, key B provided at 109. The script is ready for the execution process upon activation of the control by, e.g., a Java applet or a user clicking a button on the Web page.

The process of securely executing the script is now described with reference to Fig. 2. In one embodiment of the invention, a user running a Web browser application visits a Web site and downloads a Web page containing interactive content. The user activates a control in the

Web page, for example, by clicking on an applet. Recall from the above discussion that the control is signed at 160 with a public key digital signature using private key B 109. Thus, at 210, the signature is verified using public key B 205. Verification is accomplished by decrypting the signed control with public key B. If any change has occurred to either the control or the signature, it will be detected at 210. At 220, the script is decrypted with symmetric key 107. (Symmetric key encryption requires only one key that is shared by the encryption process and decryption process). Of course, the decryption is necessary only if the script was correspondingly encrypted at 140.

At 230, the executable commands in the script are hashed, using the same hashing function utilized at 110. The hashed commands that were encrypted and appended to the script at 120 and 130, respectively, are now decrypted at 240, using public key A, which was provided to the control at 150. The decrypted hashed commands are compared at 250 with the commands hashed at 230. If no changes in the script occurred between hashing and encrypting at 110 and 120, and hashing and decrypting at 230 and 240, the decrypted hashed commands obtained at 240 should be identical to the hashed commands obtained at 230, and the script may begin execution at 260. If, on the other hand, the commands hashed at 230 are not the same as the hashed commands decrypted at 240, the user is cautioned or warned, for example, by displaying a message in a pop up window or the like in a display screen for the client system. The user may, according to one embodiment of the invention, select to proceed with execution of the script. This is useful, for example, if a new version of the script is released, in which case hashed values for the commands in the old version of the script will not match the hashed values for the commands in the new version.

In one embodiment of the invention, the decrypted hashed commands are maintained so that a comparison between hashed command values and decrypted hashed command values may be performed before every execution of the script. Alternatively, a comparison is performed between execution of each command, to ensure there is no dynamic modification of the script or particular commands in the script. In each case, the user is warned as appropriate. In this manner, verification of the source and integrity of a script in an application, such as may be in a Web page, is accomplished.

CLAIMS

What is claimed is:

1. A method for creating a secure script, comprising:

a) generating a hashed value for at least one executable command in the script;

b) signing the hashed value to create a signed hashed value; and

c) appending the signed hashed value to the script.

2. The method of claim 1, wherein generating a hashed value for at least one executable command in the script comprises providing the executable command as a key value that is input to a mathematical function, computing the mathematical function, and providing as output from the mathematical function the hashed value.

3. The method of claim 1, wherein signing the hashed value to create a signed hashed value comprises encrypting the hashed value.

4. The method of claim 3, wherein encrypting the hashed value comprises encrypting the hashed value using a cryptographic key.

5. The method of claim 4, wherein encrypting the hashed value using a cryptographic key comprises encrypting the hashed value using a public encryption private key.

6. The method of claim 5, wherein the script is component in a World Wide Web document downloaded from a HyperText Transfer Protocol server to a client for execution thereon.

7. The method of claim 1, further comprising encrypting the script, including the signed hashed value appended to the script to create an encrypted script.

8. The method of claim 7, wherein encrypting the script comprises encrypting the script using a symmetric encryption key.

9. A method for securing a script, comprising:

a) computing a hashed value for each executable command in a script;

b) encrypting the hashed value for each executable command in the script; and

c) appending to the script the encrypted hashed values for each executable command.

10. The method of claim 9, wherein encrypting the hashed value for each executable command in the script comprises encrypting the hashed value for each executable command with a public encryption private key.

11. The method of claim 10, further comprising signing a control program, comprising the script and a public key corresponding to the private key, to keep hidden the public key.

12. The method of claim 11, wherein signing the control program comprises encrypting the control program using a second public encryption private key.

13. The method of claim 12, wherein the control program is an ActiveX control in an application program.

14. The method of claim 13, wherein the ActiveX control is in a HyperText Markup Language (HTML) document.

15. The method of claim 14, wherein the HTML document is downloaded from a HyperText Transfer Protocol (HTTP) server to a HTTP client.

16. A method for executing a script, comprising:

a) computing a hashed value for each executable command in a script;

b) decrypting an encrypted hashed value appended to the script for each executable command in the script to obtain a decrypted hashed value for each executable command in the script;

c) comparing the computed hashed value for each executable command in the script with the corresponding decrypted hashed value for each executable command in the script; and

d) executing the executable commands in the script if the computed hashed values for the executable commands in the script are the same as the corresponding decrypted hashed values appended to the script for the executable commands.

17. The method of claim 16, wherein the script is an encrypted script, further comprising decrypting the encrypted script with a symmetric encryption key to obtain the script.

18. The method of claim 16, first comprising verifying a public key cryptography signature associated with a control program comprising the script.

19. The method of claim 16, further comprising repeating a and c each execution of the executable commands in the script to prevent dynamic modification to the script.

20. The method of claim 16, wherein the script is in a HyperText Markup Language (HTML) document.

21. The method of claim 20, wherein the HTML document is downloaded to a Hypertext Transfer Protocol (HTTP) client from a HTTP server.

22. The method of claim 21 performed by an ActiveX control in the HTML document.

23. An article of manufacture comprising a machine accessible medium providing a plurality of machine readable instructions, wherein the instructions, when executed by a processor, cause the processor to:

a) compute a hashed value for each executable command in a script;

b) encrypt the hashed value for each executable command in the script; and

c) append to the script the encrypted hashed values for each executable command.

24. An article of manufacture comprising a machine accessible medium providing a plurality of machine readable instructions, wherein the instructions, when executed by a processor, cause the processor to:

a) compute a hashed value for each executable command in a script;

b) decrypt an encrypted hashed value appended to the script for each executable command in the script to obtain a decrypted hashed value for each executable command in the script;

c) compare the computed hashed value for each executable command in the script with the corresponding decrypted hashed value for each executable command in the script; and

d) execute the executable commands in the script if the computed hashed values for the executable commands in the script are the same as the corresponding decrypted hashed values appended to the script for the executable commands.

25. An apparatus, comprising:

means for computing a hashed value for each executable command in a script;

means for encrypting the hashed value for each executable command in the script; and

means for appending to the script the encrypted hashed values for each executable command.

26. An apparatus, comprising:

means for computing a hashed value for each executable command in a script;

means for decrypting an encrypted hashed value appended to the script for each executable command in the script to obtain a decrypted hashed value for each executable command in the script;

means for comparing the computed hashed value for each executable command in the script with the corresponding decrypted hashed value for each executable command in the script; and

means for executing the executable commands in the script if the computed hashed values for the executable commands in the script are the same as the corresponding decrypted hashed values appended to the script for the executable commands.

ABSTRACT OF THE DISCLOSURE

A method and apparatus for creating a secure script. Executable commands in the script are hashed, and the hashed values for the commands are encrypted and appended to the script. Before executing the script, a hashed value for each executable command in a script is computed and the encrypted hashed value appended to the script for each executable command in the script is decrypted to obtain a decrypted hashed value for each executable command in the script. The hashed value and the decrypted hashed value for each executable command is compared, and if the values are the same, the command is executed.

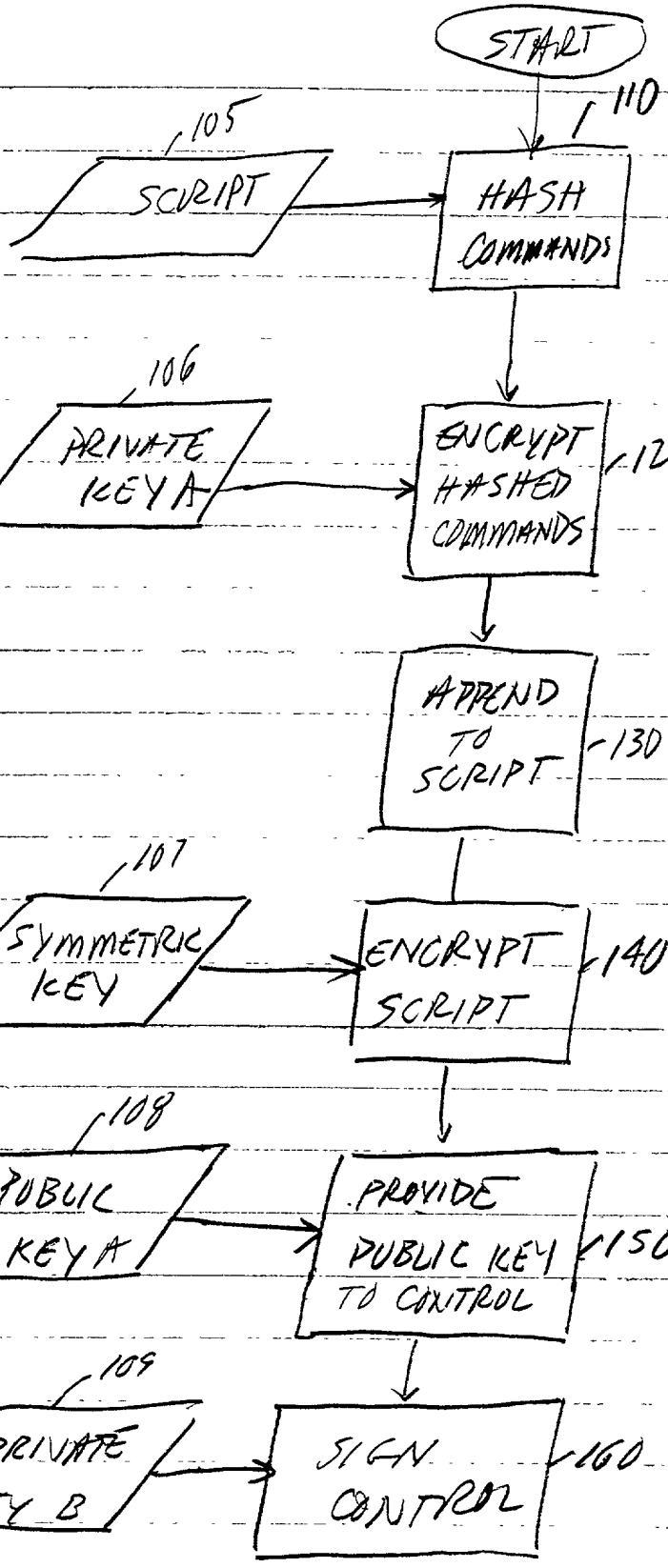
START
105
SCRIPT
110
HASH COMMANDS
106
PRIVATE KEY A
ENCRYPT HASHED COMMANDS
120
APPEND TO SCRIPT
130
107
SYMMETRIC KEY
ENCRYPT SCRIPT
140
108
PUBLIC KEY A
PROVIDE PUBLIC KEY TO CONTROL
150
109
PRIVATE KEY B
SIGN CONTROL
160

FIG 1

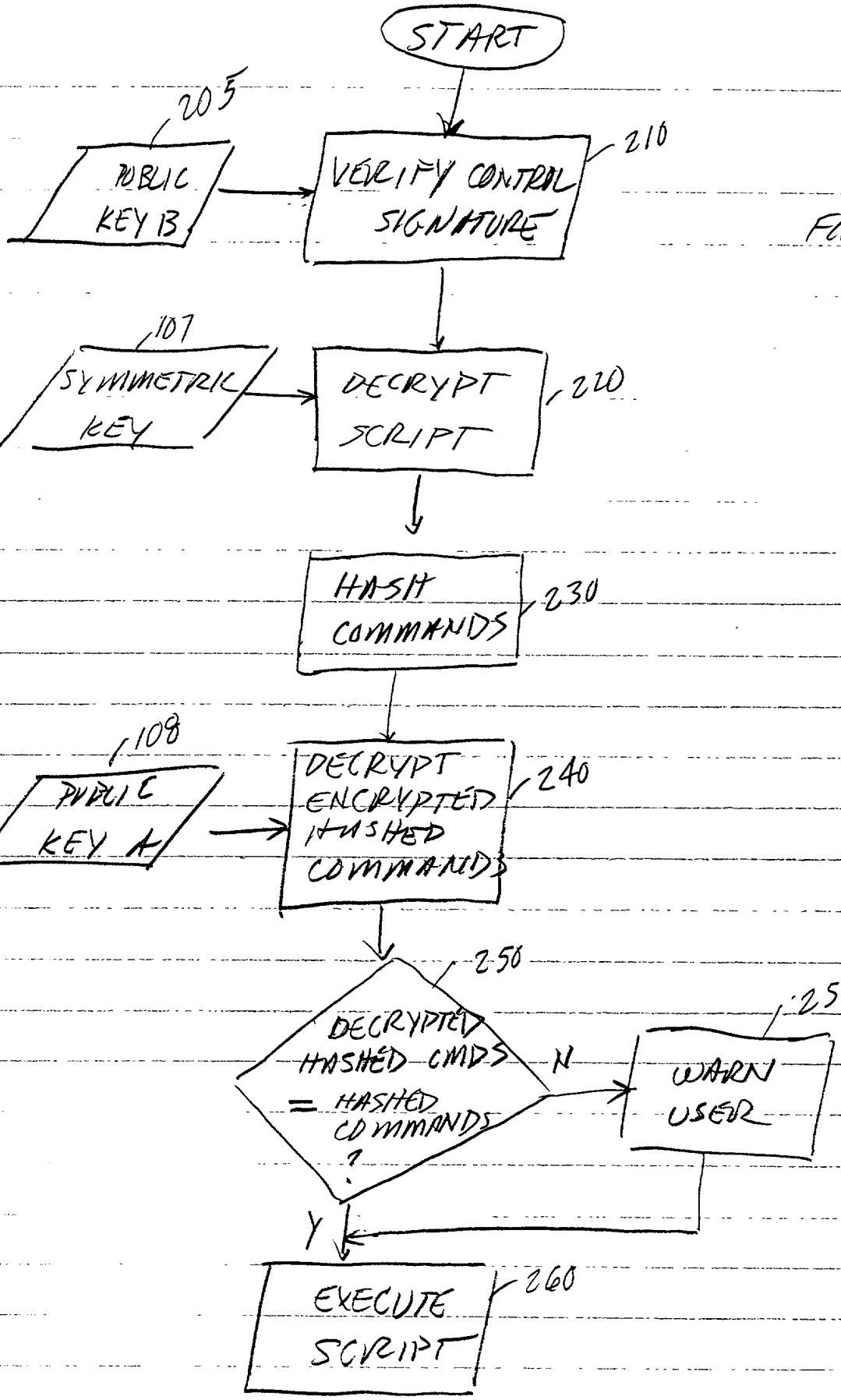
START
205
PUBLIC KEY B
VERIFY CONTROL SIGNATURE
210
107
SYMMETRIC KEY
DECRYPT SCRIPT
220
HASH COMMANDS
230
108
PUBLIC KEY A
DECRYPT ENCRYPTED HASHED COMMANDS
240
250
DECRYPTED HASHED CMDS = HASHED COMMANDS ?
N
255
WARN USER
Y
EXECUTE SCRIPT
260

FIG 2

Attorney's Docket No.: 42390.P6098 PATENT

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION
(FOR **INTEL CORPORATION** PATENT APPLICATIONS)

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below, next to my name.

I believe I am the original, first, and sole inventor (if only one name is listed below) or an original, first, and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

METHOD AND APPARATUS FOR CREATING AND EXECUTING SECURE SCRIPTS

the specification of which

XX is attached hereto.
____ was filed on _____ as
United States Application Number _____
or PCT International Application Number_____
and was amended on _____.
(if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment referred to above. I do not know and do not believe that the claimed invention was ever known or used in the United States of America before my invention thereof, or patented or described in any printed publication in any country before my invention thereof or more than one year prior to this application, that the same was not in public use or on sale in the United States of America more than one year prior to this application, and that the invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve months (for a utility patent application) or six months (for a design patent application) prior to this application.

I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d), of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)			Priority Claimed	
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No

I hereby claim the benefit under title 35, United States Code, Section 119(e) of any United States provisional application(s) listed below

(Application Number)	Filing Date
(Application Number)	Filing Date

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

(Application Number)	Filing Date	(Status -- patented, pending, abandoned)
(Application Number)	Filing Date	(Status -- patented, pending, abandoned)

I hereby appoint William E. Alford, Reg. No. 37,764; Farzad E. Amini, Reg. No. P42,261; Aloysius T. C. AuYeung, Reg. No. 35,432; William Thomas Babbitt, Reg. No. 39,591; Carol F. Barry, Reg. No. 41,600; Jordan Michael Becker, Reg. No. 39,602; Bradley J. Bereznak, Reg. No. 33,474; Michael A. Bernadicou, Reg. No. 35,934; Roger W. Blakely, Jr., Reg. No. 25,831; Gregory D. Caldwell, Reg. No. 39,926; Ronald C. Card, Reg. No. P44,587; Thomas M. Coester, Reg. No. 39,637; Donna Jo Coningsby, Reg. No. 41,684; Stephen M. De Klerk, under 37 C.F.R. § 10.9(b); Michael Anthony DeSanctis, Reg. No. 39,957; Daniel M. De Vos, Reg. No. 37,813; Robert Andrew Diehl, Reg. No. 40,992; Matthew C. Fagan, Reg. No. 37,542; Tarek N. Fahmi, Reg. No. 41,402; James Y. Go, Reg. No. 40,621; James A. Henry, Reg. No. 41,064; Willmore F. Holbrow III, Reg. No. P41,845; Sheryl Sue Holloway, Reg. No. 37,850; George W Hoover II, Reg. No. 32,992; Eric S. Hyman, Reg. No. 30,139; Dag H. Johansen, Reg. No. 36,172; William W. Kidd, Reg. No. 31,772; Erica W. Kuo, Reg. No. 42,775; Michael J. Mallie, Reg. No. 36,591; Andre L. Marais, under 37 C.F.R. § 10.9(b); Paul A. Mendonsa, Reg. No. 42,879; Darren J. Milliken, Reg. 42,004; Lisa A. Norris, Reg. No. P44,976; Chun M. Ng, Reg. No. 36,878; Thien T. Nguyen, Reg. No. 43,835; Thinh V. Nguyen, Reg. No. 42,034; Dennis A. Nicholls, Reg. No. 42,036; Kimberley G. Nobles, Reg. No. 38,255; Daniel E. Ovanezian, Reg. No. 41,236; Babak Redjaian, Reg. No. 42,096; William F. Ryann, Reg. 44,313; James H. Salter, Reg. No. 35,668; William W. Schaal, Reg. No. 39,018; James C. Scheller, Reg. No. 31,195; Jeffrey Sam Smith, Reg. No. 39,377; Maria McCormack Sobrino, Reg. No. 31,639; Stanley W. Sokoloff, Reg. No. 25,128; Judith A. Szepesi, Reg. No. 39,393; Vincent P. Tassinari, Reg. No. 42,179; Edwin H. Taylor, Reg. No. 25,129; John F. Travis, Reg. No. 43,203; George G. C. Tseng, Reg. No. 41,355; Joseph A. Twarowski, Reg. No. 42,191; Lester J. Vincent, Reg. No. 31,460; Glenn E. Von Tersch, Reg. No. 41,364; John Patrick Ward, Reg. No. 40,216; Charles T. J. Weigell, Reg. No. 43,398; Kirk D. Williams, Reg. No. 42,229; James M. Wu, Reg. No. P45,241; Steven D. Yates, Reg. No. 42,242; Ben J. Yorks, Reg. No. 33,609; and Norman Zafman, Reg. No. 26,250; my patent attorneys, and Andrew C. Chen, Reg. No. 43,544; Justin M. Dillon, Reg. No. 42,486; Paramita Ghosh, Reg. No. 42,806; and Sang Hui Kim, Reg. No. 40,450; my patent agents, of BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP, with offices located at 12400 Wilshire Boulevard, 7th Floor, Los Angeles, California 90025, telephone (310) 207-3800, and Alan K. Aldous, Reg. No. 31,905; Robert D. Anderson, Reg. No. 33,826; Joseph R. Bond, Reg. No. 36,458; Richard C. Calderwood, Reg. No. 35,468; Jeffrey S. Draeger, Reg. No. 41,000; Cynthia Thomas Faatz, Reg No. 39,973; Sean Fitzgerald, Reg. No. 32,027; John N Greaves, Reg. No. 40,362; Seth Z. Kalson, Reg. No. 40,670; David J. Kaplan, Reg. No. 41,105; Charles A. Mirho, Reg. No. 41,199; Leo V. Novakoski, Reg. No. 37,198; Naomi Obinata, Reg. No. 39,320; Thomas C. Reynolds, Reg. No. 32,488; Kenneth M. Seddon, Reg. No. 43,105; Mark Seeley, Reg. No. 32,299; Steven P. Skabrat, Reg. No. 36,279; Howard A. Skaist, Reg. No. 36,008; Steven C. Stewart, Reg. No. 33,555; Raymond J. Werner, Reg. No. 34,752; Robert G. Winkle, Reg. No. 37,474; and Charles K. Young, Reg. No. 39,435; my patent attorneys, and Thomas Raleigh Lane, Reg. No. 42,781; Calvin E. Wells; Reg. No. P43,256, Peter Lam, Reg. No. P44,855; and Gene I. Su, Reg. No. 45,140; my patent agents, of INTEL CORPORATION; and James R. Thein, Reg. No. 31,710, my patent attorney; with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.

Send correspondence to Gregory D. Caldwell, BLAKELY, SOKOLOFF, TAYLOR
(Name of Attorney or Agent)
& ZAFMAN LLP, 12400 Wilshire Boulevard 7th Floor, Los Angeles, California 90025
and direct telephone calls to Gregory D. Caldwell, (503) 684-6200.
(Name of Attorney or Agent)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Sole/First Inventor Rodney A. Korn

Inventor's Signature _____ Date _____

Residence Redmond, Washington (City, State) Citizenship United States (Country)

Post Office Address 15127 NE 24th street, PMB 400
Redmond, Washington 98052